UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/066,367	01/31/2002	Robert David Zobel	05456.105009	2476

7590 07/14/2005

Robert T. Neufeld, Esq.
KING & SPALDING
45th Floor
191 Peachtree Street, N.E.
Atlanta, GA 30303

EXAMINER	
SHAW, YIN CHEN	

ART UNIT	PAPER NUMBER
2135	

DATE MAILED: 07/14/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/066,367	ZOBEL ET AL.	
	Examiner	Art Unit	
	Yin-Chen Shaw	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *31 January 2002*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-45* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-45* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *31 January 2002* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *08/2002-05/2003*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-45 have been submitted for examination.
2. Claims 1-45 have been examined and rejected.

Priority

3. The application has been filed under Title 35 U.S.C. 119(e), claiming priority to provisional application 60/265,519, filed on Jan. 31, 2001.
4. The effective filing data for the subject matter defined in the pending claims in this application is Jan. 31, 2001.

Claim Interpretation

5. Claims have been afforded their broadest reasonable interpretation. Applicant's language directed to audit scan that is more thorough is interpreted as scan related to specific object and its associated registry. The word, configuring, is interpreted as equivalent to making different selections among the available options either manually or automatically. The asset value is interpreted as equivalent to the priority value associated with the devices in the network environment.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

6. Claims 30, 32, 34-35, and 37-38 are rejected under 35 U.S.C. 103(a) as being unpatentable over Proctor (U.S. Patent 6,530,024) and further in view of Gleichauf et al. (U.S. Patent 6,301,668).

   a. *Referring to Claim 30:*

      As per Claim 30, Proctor discloses a method for assessing the security of a network comprising the steps of:

      selecting an audit scan to perform on the network element, said selection based on the initial scan **[i.e., Object audit 324 can include an identification of one or more objects 322 to which the audit pertains, a user or users 326 whose activities should be audited with respect to identified objects, and operations 328 performed or attempted on the identified object or objects (lines 56-61, Col 7). Registry key audit 334 can include an identification of a list 332 of one or more registry keys to be audited, a user or user 336 whose activities should be audited, a user or user 336 whose activities should be audited with respect to identified files, and operations 338 performed or attempted on the identified registry keys (lines 63-67, Col. 7). One example implementation of creating an object audit is illustrated n**

FIG. 5 (lines 18-20, Col. 8), where the type of object audit is subjected to edition and modification. FIG. 6 is a diagram of a computer screen illustrating an example implementation of a registry key audit according to one embodiment of the invention. Registry key list window portion 604 allows a selection of one or more registry keys for the system of interest. Add, edit and remove buttons 609 can be used to update and create the registry key list (lines 1-7, Col. 9)];

performing the selected audit scan on the network **[i.e., The auditing performed can include monitoring the networked computing environment for the occurrence of the identified activities for the users or groups of users (lines 10-12, Col. 2)]**.

receiving data from the selected audit scan of the network element **[i.e., Collection policies are policies that set forth the specific details on how or when the auditing information is to be collected (lines 29-30, Col. 9)]**; and

computing a security score for the network element from the selected audit scan **[i.e., The collected records are provided to the security system for analysis. This analysis is referred to as a security assessment 924. In a step 1052, the security assessment is performed based on the audited activities that**

have been recorded in event log files 908 (lines 41-45, Col. 11)].

Proctor does not expressly disclose the remaining limitations of the claim. However, Gleichauf et al. disclose receiving an initial scan identifying a network element **[i.e., Scan engine 22 can direct requests upon the network and assess responses to such request to discover network information (lines 52-54, Col. 5). Such network information could comprise the devices coupled to internal network 10, the operating systems running on such devices and the services available on each device (lines 59-62, Col. 5)]**. Proctor and Gleichauf et al. are analogous art because they are from similar technology relating to the security and scanning process of the computer system. It would have been obvious to one of ordinary skill in the art at the time of invention was made to have a scanning system capable of providing different scope of scanning functions by combining the network scan Gleichauf et al. with the object and registry scans from Proctor since one would have been motivated to have a security product **function in an environment wherein the traffic exceeds their memory or processor capacity (lines, 34-36, Col. 2)**. Therefore, it would have been obvious to modify Proctor with Gleichauf et al. to obtain the invention as specified in Claim 30.

b. *Referring to Claim 32:*

As per Claim 32, Proctor and Gleichauf et al. disclose the method of claim 30. In addition, Proctor discloses modifying the selected audit scan, said modification based on the data received from the selected audit scan **[i.e., The collected records are provided to the security system for analysis. This analysis is referred to as a security assessment 924. In a step 1052, the security assessment is performed based on the audited activities that have been recorded in event log files 908 (lines 41-45, Col. 11). When security assessment 924 determines that an actual attempted or potential security breach has occurred or is occurring, one or more policy updates 928 are made to on or more of the audit policy 904, collection policy 912, and detection policy 916 (lines 49-53, Col. 11)]**.

c. *Referring to Claim 34:*

As per Claim 34, it encompasses limitations that are similar to those of Claim 30. Thus, it is rejected with the same rationale applied against Claim 30 above.

d. *Referring to Claim 35:*

As per Claim 35, Proctor and Gleichauf et al. disclose the method of claim 30, wherein the step of selecting an audit scan is based on a manual input **[i.e., One example implementation of creating an object audit is illustrated n FIG. 5 (lines 18-20,**

Col. 8), where the type of object audit is subjected to edition and modification. FIG. 6 is a diagram of a computer screen illustrating an example implementation of a registry key audit according to one embodiment of the invention. Registry key list window portion 604 allows a selection of one or more registry keys for the system of interest. Add, edit and remove buttons 609 can be used to update and create the registry key list (lines 1-7, Col. 9)].

e. *Referring to Claim 37:*

As per Claim 37, Proctor and Gleichauf et al. disclose the method of claim 30. In addition, Proctor discloses the step of computing a security score as in claim 30. Proctor and Gleichauf et al. do not expressly disclose summing one or more vulnerabilities associated with the element. However, Proctor discloses the assessment of potential security breach based on the audited activities **[i.e., In a step 1052, the security assessment is performed based on the audited activities that have been recorded in event log files 908 (lines 43-45, Col. 11). When security assessment 924 determines that an actual attempted or potential security breach has occurred or is occurring, one or more policy updates 928 are made to on or more of the audit policy 904, collection policy 912, and detection policy 916 (lines 49-53, Col. 11). In a step 1104, the user or**

group of users associated with the potential security breach are identified. As described, this identification can come from the audited information in which activities for a user or groups of users are tracked and recorded according to the defined user or groups of users (lines 56-61, Col. 11)], and Gleichauf et al. disclose identifying the potential vulnerabilities of the network **[i.e., Additionally, in the embodiment of FIG. 1, scan engine 22 is operable to analyze the network information to identify potential vulnerabilities of internal network 10 (lines 62-65, Col. 15)]**. Proctor and Gleichauf et al. are analogous art because they are from similar technology relating to the security and scanning process of the computer system. It would have been obvious to one of ordinary skill in the art at the time of invention was made to combine Proctor with Gleichauf et al. to formulate the assessments from the scans for an accurate determination of the security of the network and its elements since one would have been motivated to avoid the situation where **a lack of network information compromises the security product's ability to detect such attacks such as insertion attacks, evasion attacks and denial of service attacks (lines 58-60, Gleichauf et al.)**. Therefore, it would have been obvious to modify Proctor with Gleichauf et al. to obtain the invention as specified in Claim 37.

f. *Referring to Claim 38:*

As per Claim 38, Proctor and Gleichauf et al. disclose the steps recited in claim 30. In addition, Proctor discloses a computer-readable medium having computer-executable instructions **[i.e., FIG. 15 is a block diagram illustrating a general purpose computer system, including examples of computer readable media for providing computer software or instructions to perform the functionality described herein (lines 11-14, Col. 17)]**.

7. Claim 31 is rejected under 35 U.S.C. 103(a) as being unpatentable over Proctor (U.S. Patent 6,530,024) and Gleichauf et al. (U.S. Patent 6,301,668) as applied to claim 30 above, and further in view of Hartley et al. (U.S. Patent 6,889,168).

a. *Referring to Claim 31:*

As per Claim 31, Proctor and Gleichauf et al. disclose the method of claim 30. Proctor and Gleichauf et al. do not expressly disclose the step of scheduling the selected audit scan, said scheduling based on the initial scan. However, Hartley et al. disclose the scheduling module which is used for specifying the time of conducting security modules or all the test **[i.e., The schedule module 32 provides the functionality to run security checks at predetermined intervals. Checks can be scheduled to run**

at specific designated times as well as at regular intervals such as monthly or weekly. The schedule module further provides the flexibility to run individual security modules or all tests (lines 9-14, Col. 7). A variety of further screens may be presented which provide the system user the choices of one or more modules scheduled, the data which the function will be performed. Further options may be provided such as periodic activation of the functions, one time activations of the functions, or the combination of various security and utility modules (lines31-38, Col. 10)]. Proctor, Gleichauf et al., and Hartley et al. are analogous art because they are from similar technology relating to the security and scanning process of the computer system. It would have been obvious to one of ordinary skill in the art at the time of invention was made to combine Proctor and Gleichauf et al. with Hartley et al. to have the initial scan scheduled prior to the audit scan since one would be motivated **to protect the information stored on server from unauthorized access (lines 49-50, Col. 1, Hartley et al.)**. Therefore, it would have been obvious to modify Proctor and Gleichauf et al. with Hartley et al. to obtain the invention as specified in Claim 31.

8. Claims 1-2, 4-5, 9, 11-15, 17, 20-23, 25-26, 28-29, 39, 42-45 are rejected under 35 U.S.C. 103(a) as being unpatentable over Proctor (U.S. Patent 6,530,024) and further in view of Gleichauf et al. (U.S. Patent 6,301,668) and Hartley et al. (U.S. Patent 6,889,168).

   a. *Referring to Claim 1:*

      As per Claim 1, Proctor discloses a computer-implemented method for configuring a security audit of a computer network **[i.e., a networked computing environment (line 67, Col. 4)]** comprising the steps of:

      configuring an audit scan to perform on the element, wherein the audit scan is a more thorough scan than the element **[i.e., Object audit 324 can include an identification of one or more objects 322 to which the audit pertains, a user or users 326 whose activities should be audited with respect to identified objects, and operations 328 performed or attempted on the identified object or objects (lines 56-61, Col 7). Registry key audit 334 can include an identification of a list 332 of one or more registry keys to be audited, a user or user 336 whose activities should be audited, a user or user 336 whose activities should be audited with respect to identified files, and operations 338 performed or attempted on the identified registry keys (lines 63-67, Col. 7). One example implementation of creating an object audit is illustrated n**

FIG. 5 (lines 18-20, Col. 8), where the type of object audit is subjected to edition and modification. FIG. 6 is a diagram of a computer screen illustrating an example implementation of a registry key audit according to one embodiment of the invention. Registry key list window portion 604 allows a selection of one or more registry keys for the system of interest. Add, edit and remove buttons 609 can be used to update and create the registry key list (lines 1-7, Col. 9)];

calculating a security score for the element based on the audit scan **[i.e., The collected records are provided to the security system for analysis. This analysis is referred to as a security assessment 924. In a step 1052, the security assessment is performed based on the audited activities that have been recorded in event log files 908 (lines 41-45, Col. 11)]**.

Proctor discloses performing the audit scan on the element **[i.e., The auditing performed can include monitoring the networked computing environment for the occurrence of the identified activities for the users or groups of users (lines 10-12, Col. 2)]**.

Proctor does not expressly disclose the scheduling feature regarding to the audit scan. However, Hartley et al. disclose the scheduling module which is used for specifying the time of conducting security modules or all the test **[i.e., The schedule**

module 32 provides the functionality to run security checks at predetermined intervals. Checks can be scheduled to run at specific designated times as well as at regular intervals such as monthly or weekly. The schedule module further provides the flexibility to run individual security modules or all tests (lines 9-14, Col. 7). A variety of further screens may be presented which provide the system user the choices of one or more modules scheduled, the data which the function will be performed. Further options may be provided such as periodic activation of the functions, one time activations of the functions, or the combination of various security and utility modules (lines31-38, Col. 10)]. In addition, Gleichauf et al. disclose conducting a discovery scan to identify an element of the computer network and determine the element's functions **[i.e., Scan engine 22 can direct requests upon the network and assess responses to such request to discover network information (lines 52-54, Col. 5). Such network information could comprise the devices coupled to internal network 10, the operating systems running on such devices and the services available on each device (lines 59-62, Col. 5)]** and scanning process can be repeated **[i.e., At step 124 it is determined if the scanning steps should be repeated. If so, the method returns to step 100 to obtain updated network**

information, and the method is repeated (lines 12-14, Col. 9)]. Proctor, Gleichauf et al., and Hartley et al. are analogous art because they are from similar technology relating to the security and scanning process of the computer system. It would have been obvious to one of ordinary skill in the art at the time of invention was made to combine Proctor with Hartley et al. to have (1) scheduling a time to perform the audit scan on the element, (2) running the audit scan of the element at the scheduled time, and (3) scheduling another time to repeat the audit scan on the element, the scheduling based on the results of the audit scan, and with Gleichauf et al. to have the different scope of scanning capability for the system since one would have been motivated to have a security product **function in an environment wherein the traffic exceeds their memory or processor capacity (lines, 34-36, Col. 2, Gleichauf et al.)** and **to protect the information stored on server from unauthorized access (lines 49-50, Col. 1, Hartley et al.)**. Therefore, it would have been obvious to modify Proctor with Gleichauf et al. and Hartley et al. to obtain the invention as specified in Claim 1.

b. *Referring to Claim 2:*

As per Claim 2, Proctor, Gleichauf et al., and Hartley et al. disclose the method of claim 1. In addition, Proctor discloses the step of configuring a subsequent audit scan of the element that is

different from the audit scan **[i.e., One example implementation of creating an object audit is illustrated in FIG. 5 (lines 18-20, Col. 8), where the type of object audit can be subjected to variety of edition and modification. FIG. 6 is a diagram of a computer screen illustrating an example implementation of a registry key audit according to one embodiment of the invention. Registry key list window portion 604 allows a selection of one or more registry keys for the system of interest. Add, edit and remove buttons 609 can be used to update and create the registry key list (lines 1-7, Col. 9)]**.

c. *Referring to Claim 4:*

As per Claim 4, the rejection of Claim 1 is incorporated. In addition, Claim 4 encompasses the same limitations that are similar to those of Claim 1. Thus, it is rejected with the same rationale applied against Claim 1 above.

d. *Referring to Claim 5:*

As per Claim 5, Proctor, Gleichauf et al., and Hartley et al. disclose the method of claim 1. In addition, Gleichauf et al. disclose wherein the step of conducting a discovery scan further comprises identifying vulnerabilities associated with the element **[i.e., In step 108, the potential vulnerabilities discovered in step 106 are confirmed, for example by executing active**

exploits on the network against the potential vulnerabilities (lines 15-18, Col. 8)].

e. *Referring to Claim 9:*

As per Claim 9, Proctor, Gleichauf et al., and Hartley et al. disclose the method of claim 1. Proctor, Gleichauf et al., and Hartley et al. do not expressly disclose wherein the step of configuring an audit scan comprises selecting a type of audit scan based on the discovery scan. However, Proctor discloses configuring an audit scan as in Claim 1. In addition, Gleichauf et al. disclose the discovery scan as in Claim 1. Proctor, Gleichauf et al., and Hartley et al. are analogous art because they are from similar technology relating to the security and scanning process of the computer system. It would have been obvious to one of ordinary skill in the art at the time of invention was made to combine Proctor with Gleichauf et al. to have an audit scan process selected based on the prior discovery scan since one would have been motivated to **have a increased security measure as users became more sophisticated (lines 36 and 43, Col 1)**. Therefore, it would have been obvious to modify Proctor with Gleichauf et al. and Hartley et al. to obtain the invention as specified in Claim 9.

f. *Referring to Claim 11:*

As per Claim 11, Proctor, Gleichauf et al., and Hartley et al. disclose the method of claim 1. In addition, Proctor discloses wherein the step of configuring an audit scan comprises manually selecting the type of audit scan **[i.e., One example implementation of creating an object audit is illustrated n FIG. 5 (lines 18-20, Col. 8), where the type of object audit can be subjected to variety of edition and modification. Although the functionality is not illustrated on the screen diagram of FIG. 5, the functionality can be provided in one embodiment to allow the administrator to create and edit custom groups (lines 50-53, Col. 8). FIG. 6 is a diagram of a computer screen illustrating an example implementation of a registry key audit according to one embodiment of the invention. Registry key list window portion 604 allows a selection of one or more registry keys for the system of interest. Add, edit and remove buttons 609 can be used to update and create the registry key list (lines 1-7, Col. 9). Additionally, the administrator can select whether to replace auditing on existing sub keys as illustrated by selection box 614 (lines 16-18, Col 9)]**.

g. *Referring to Claim 12:*

As per Claim 12, Proctor, Gleichauf et al., and Hartley et al. disclose the steps recited in claim 1. In addition, Proctor

discloses a computer-readable medium having computer-executable instructions **[i.e., FIG. 15 is a block diagram illustrating a general purpose computer system, including examples of computer readable media for providing computer software or instructions to perform the functionality described herein (lines 11-14, Col. 17)]**.

h. *Referring to Claim 13:*

As per Claim 13, it encompasses limitations that are similar to those of Claim 1. Thus, it is rejected with the same rationale applied against Claim 1 above.

i. *Referring to Claim 14:*

As per Claim 14, it encompasses limitations that are similar to those of Claim 1. Thus, it is rejected with the same rationale applied against Claim 1 above.

j. *Referring to Claim 15:*

As per Claim 15, it encompasses limitations that are similar to those of Claim 1. Thus, it is rejected with the same rationale applied against Claim 1 above.

k. *Referring to Claim 17:*

As per Claim 17, the rejection of Claim 13 is incorporated. In addition, Claim 17 encompasses limitations that are similar to those of Claim 4 and 5. Thus, it is rejected with the same rationale applied against Claim 4 and 5 above.

l. *Referring to Claim 20:*

As per Claim 20, the rejection of Claim 13 is incorporated. In addition, Claim 20 encompasses limitations that are similar to those of Claim 11. Thus, it is rejected with the same rationale applied against Claim 11 above.

m. *Referring to Claim 21:*

As per Claim 21, it encompasses limitations that are similar to those of Claim 12. Thus, it is rejected with the same rationale applied against Claim 12 above.

n. *Referring to Claim 22:*

As per Claim 22, it encompasses limitations that are similar to those of Claim 1 and 30. Thus, it is rejected with the same rationale applied against Claim 1 and 30 above.

o. *Referring to Claim 23:*

As per Claim 23, the rejection of Claim 22 is incorporated. In addition, Claim 23 encompasses limitations that are similar to those of Claim 32. Thus, it is rejected with the same rationale applied against Claim 32 above.

p. *Referring to Claim 25:*

As per Claim 25, it encompasses limitations that are similar to those of Claim 22. Thus, it is rejected with the same rationale applied against Claim 22 above.

q. *Referring to Claim 26:*

As per Claim 26, the rejection of Claim 22 is incorporated. In addition, Claim 26 encompasses limitations that are similar to those of Claim 35. Thus, it is rejected with the same rationale applied against Claim 35 above.

r. *Referring to Claim 28:*

As per Claim 37, the rejection of Claim 30 is incorporated. In addition, Claim 37 encompasses limitations that are similar to those of Claim 28. Thus, it is rejected with the same rationale applied against Claim 28 above.

s. *Referring to Claim 29:*

As per Claim 29, Proctor, Gleichauf et al., and Hartley et al. disclose the steps recited in claim 22. In addition, Proctor discloses a computer-readable medium having computer-executable instructions **[i.e., FIG. 15 is a block diagram illustrating a general purpose computer system, including examples of computer readable media for providing computer software or instructions to perform the functionality described herein (lines 11-14, Col. 17)]**.

t. *Referring to Claim 39:*

As per Claim 39, Proctor discloses a system for configuring **[i.e., One example implementation of creating an object audit is illustrated n FIG. 5 (lines 18-20, Col. 8), where the type of object audit is subjected to edition and modification. FIG. 6**

is a diagram of a computer screen illustrating an example implementation of a registry key audit according to one embodiment of the invention. Registry key list window portion 604 allows a selection of one or more registry keys for the system of interest. Add, edit and remove buttons 609 can be used to update and create the registry key list (lines 1-7, Col. 9)] a security audit of a computer network comprising the computer network **[i.e., a computer network (line 3, Col. 5)]**. Proctor further discloses a console operable for receiving and transmitting information about the audit scan **[i.e., Security procedures can also be applied to security console 104B (lines 42-43, Col. 5). In one embodiment, the security procedures can include for example, one or more of security policies, collection policies, detection policies and audit policies. The security console 104B can also perform the adaptive feedback operations, including updating the security procedures based on security occurrences (lines 45-47, Col. 5). The example embodiment illustrated in FIG. 3, the audit policy 300 includes a system audit 304, and object audit 324, and a registry key audit 334 (lines 48-50, Col. 7)]**. Proctor does not expressly disclose a discovery scan and scheduling feature associated with different types of scans, However, Gleichauf et al. disclose a security audit system **[i.e.,**

network security system 20 (line 16, Col. 5)] operable for conducting a discovery scan to identify an element of the computer network **[i.e., Scan engine 22 can direct requests upon the network and assess responses to such requests to discover network information (lines 52-54, Col. 5)]**. In addition, Hartley disclose the scheduling module which is used for specifying the time of conducting security modules or all the test **[i.e., The schedule module 32 provides the functionality to run security checks at predetermined intervals. Checks can be scheduled to run at specific designated times as well as at regular intervals such as monthly or weekly. The schedule module further provides the flexibility to run individual security modules or all tests (lines 9-14, Col. 7)]**. Proctor, Gleichauf et al., and Hartley et al. are analogous art because they are from similar technology relating to the security and scanning process of the computer system. It would have been obvious to one of ordinary skill in the art at the time of invention was made to combine Proctor with Hartley et al. to have a system with scheduling feature for the audit scan a time to perform the audit scan on the element, and with Gleichauf et al. to have the scanning process performed at different scope for the system by communicating through the console since one would have been motivated to have a security product **function in an environment**

wherein the traffic exceeds their memory or processor capacity (lines, 34-36, Col. 2, Gleichauf et al.) and **to protect the information stored on server from unauthorized access (lines 49-50, Col. 1, Hartley et al.)**. Therefore, it would have been obvious to modify Proctor with Gleichauf et al. and Hartley et al. to obtain the invention as specified in Claim 39.

u. *Referring to Claim 42:*

As per Claim 42, Proctor, Gleichauf et al., and Hartley et al. disclose the system of claim 39. In addition, Gleichauf et al. disclose wherein the security audit system further comprises a system scanning engine operable for detecting particular vulnerabilities on the network element **[i.e., Additionally, in the embodiment of FIG. 1, scan engine 22 is operable to analyze the network information to identify potential vulnerabilities of internal network 10 (lines 62-65, Col. 15)]**.

v. *Referring to Claim 43:*

As per Claim 43, Proctor, Gleichauf et al., and Hartley et al. disclose the system of claim 39. In addition, Gleichauf et al. disclose wherein the security audit system further comprises an Internet scanning engine operable for performing a discovery scan on the network **[i.e., Scan engine 22 can direct request upon the network and assess responses to such requests to discover network information. In one embodiment, scan**

engine 22 scans devices on internal network, such as workstations 12. For example, Scan engine 22 could ping devices on internal network 10 and then perform port scans on each device. Banners from the port scans could be collected and analyzed to discover network information (lines 52-59, Col. 5)].

w. *Referring to Claim 44:*

As per Claim 44, Proctor, Gleichauf et al., and Hartley et al. disclose the system of claim 39. In addition, Gleichauf et al. disclose the security audit system. Gleichauf et al. do not expressly disclose the remaining limitations of the claim. However, Hartley et al. disclose a database scanning engine operable for detecting vulnerabilities in database elements within the network **[i.e., The integrity checker module 22 performs an analysis of the computer system in order to find security holes located therein. The analysis performed may find vulnerabilities in such things as: the type of computer/operating system used, the access privileges of files, the owner of the files, the group of the files, the date of the files, or a version number for a send mail program (lines 36-42, Col. 5)]**. Proctor, Gleichauf et al., and Hartley et al. are analogous art because they are from similar technology relating to the security and scanning process of the computer system. It

would have been obvious to one of ordinary skill in the art at the time of invention was made to combine Proctor with Gleichauf et al. and Hartley et al. to have scanning engine for analyzing the vulnerability relating to the software files since one would have been motivated to have a security product **function in an environment wherein the traffic exceeds their memory or processor capacity (lines, 34-36, Col. 2, Gleichauf et al.)** and **to protect the information stored on server from unauthorized access (lines 49-50, Col. 1, Hartley et al.)**. Therefore, it would have been obvious to modify Proctor with Gleichauf et al. and Hartley et al. to obtain the invention as specified in Claim 44.

x. *Referring to Claim 45:*

As per Claim 45, Proctor, Gleichauf et al., and Hartley et al. disclose the system of claim 39. Gleichauf et al. further disclose the security audit system and the discovery scan, Gleichauf et al. do not expressly disclose the remaining limitations of the claim. However, Proctor discloses the audit scan as in Claim 1. In addition, Hartley et al. disclose an active scan engine **[i.e., The security system processing module 15 (line13-14, Col. 4)]** operable for selecting, coordinating, and scheduling various scans to be performed on the computer network. Proctor, Gleichauf et al., and Hartley et al. are analogous art because they are from

similar technology relating to the security and scanning process of the computer system. It would have been obvious to one of ordinary skill in the art at the time of invention was made to combine Proctor with Gleichauf et al. and Hartley et al. to have the active security system processing module managing the scanning processes from Proctor and Gleichauf et al. since one would have been motivated to have a security product **function in an environment wherein the traffic exceeds their memory or processor capacity (lines, 34-36, Col. 2, Gleichauf et al.)** and **to protect the information stored on server from unauthorized access (lines 49-50, Col. 1, Hartley et al.)**. Therefore, it would have been obvious to modify Proctor with Gleichauf et al. and Hartley et al. to obtain the invention as specified in Claim 45.

9. Claim 33 is rejected under 35 U.S.C. 103(a) as being unpatentable over Proctor (U.S. Patent 6,530,024) and Gleichauf et al. (U.S. Patent 6,301,668) as applied to claim 30 above, and further in view of Yang (U.S. Patent 6,467,002)

   a. *Referring to Claim 33:*

      As per Claim 33, Proctor amd Gleichauft et al. disclose the method of claim 30. In addition, Gleichauf et al. disclose wherein the step of receiving an initial scan comprises:

identifying an operating system and a service for the network element, and identifying a vulnerability associated with the network element **[i.e., Scan engine 22 can direct requests upon the network and assess responses to such requests to discover network information (lines 52-54, Col. 5). Such network information could comprise the devices coupled to internal network 10, the operating systems running on such devices, and the services available on each device. Additionally, in the embodiment of FIG.1, scan engine 22 is operable to analyze the network information to identify potential vulnerabilities of internal network 10, and confirm these potential vulnerabilities (lines 59-65, Col. 5)]**. Gleichauf et al. do not expressly disclose determining an asset value of the network element from the operating system and the service of the network element. However, Yang discloses a priority assignment module for assigning priority values to various devices in the network environment **[i.e., Specifically, in one embodiment, the present invention assigns an initial priority order to the plurality of devices such tat those devices have priorities which are distinct (lines 44-46, Col. 2). Thus, the present invention is highly conducive for use with existing computer systems and/or networks (lines 4-6, Col. 10)]**. Proctor, Gleichauf et al., and Yang are analogous art because they are

from similar technology relating to the computer system linked in the network. It would have been obvious to one of ordinary skill in the art at the time of invention was made to modify Proctor, Gleichauf et al. with Yang to have the function of the priority assignment based on the operating system and the services of the network element incorporated into the priority engine since one would have been motivated to **realize that an efficient mechanism for priority arbitration is much needed in such a shred-resource environment in order to optimize the performance of computer systems and networks (lines 43-46, Col. 1, Yang)**. Therefore, it would have been obvious to modify Proctor and Gleichauf et al. with Yang to obtain the invention as specified in Claim 33.

10. Claims 3, 16, 27, and 41 are rejected under 35 U.S.C. 103(a) as being unpatentable over Proctor (U.S. Patent 6,530,024), Gleichauf et al. (U.S. Patent 6,301,668), and Hartley et al. (U.S. Patent 6,889,168) as applied to claims 1, 13, 22, and 39 above, and further in view of Brabson et al. (U.S. Patent 5,715,395)

    a. *Referring to Claim 3:*

    As per Claim 3, Proctor, Gleichauf et al., and Hartley et al. disclose the method of claim 1. Proctor, Gleichauf et al., and Hartley et al. do not explicitly disclose the step of receiving a

blackout time during which no audit scan can be scheduled. However, Brabson et al. disclose that network can be scheduled to be unavailable due to the scheduled maintenance and appropriate method would be utilized to provide this information to the network node **[i.e., a particular portion of a network was scheduled to be unavailable for scheduled maintenance it would supply appropriate values for the UNAVAILABILITY PERIOD to the Network nodes. If the UNAVAILABILITY PERIOD information is stored in a table at the originating node the network manager could update the table as required (lines 23-28, Col. 11)]**. Proctor, Gleichauf et al., Hartley et al., and Barbson are analogous art because they are from similar technology relating to the network and computer system. It would have been obvious to one of ordinary skill in the art at the time of invention was made to combine Proctor, Gleichauf et al. Hartley et al., and Brabson et al. to have the schedule module providing time information regarding to scheduled scanning tasks and the blackout time due to network maintenance since one would have been motivated to reduce **the impact of network resource location traffic when resources become unavailable, unreachable, or unlocatable (lines 65-67, Col. 3)**. Therefore, it would have been obvious to modify Proctor,

Gleichauf et al., and Hartley et al. with Brabson et al. to obtain the invention as specified in Claim 33.

b. *Referring to Claim 16:*

As per Claim 16, the rejection of Claim 13 is incorporated. In addition, Claim 16 encompasses limitations that are similar to those of Claim 3. Thus, it is rejected with the same rationale applied against Claim 3 above.

c. *Referring to Claim 27:*

As per Claim 27, Proctor, Gleichauf et al., and Hartley et al. disclose the method of claim 22. Proctor, Gleichauf et al., and Hartley et al. do not explicitly disclose the step of receiving a blackout time during which no audit scan can be scheduled. However, Brabson et al. disclose that network can be scheduled to be unavailable due to the scheduled maintenance and appropriate method would be utilized to provide this information to the network node for the network manager to be aware **[i.e., Thus, if the network manager was aware that a particular portion of a network was scheduled to be unavailable for scheduled maintenance it would supply appropriate values for the UNAVAILABILITY PERIOD to the Network nodes. If the UNAVAILABILITY PERIOD information is stored in a table at the originating node the network manager could update the table as required (lines 22-28, Col. 11)]**. Proctor, Gleichauf

et al., Hartley et al., and Barbson are analogous art because they are from similar technology relating to the network and computer system. It would have been obvious to one of ordinary skill in the art at the time of invention was made to combine Proctor, Gleichauf et al. Hartley et al., and Brabson et al. to have the schedule module providing time information regarding to scheduled scanning tasks and the blackout time due to network maintenance since one would have been motivated to reduce **the impact of network resource location traffic when resources become unavailable, unreachable, or unlocatable (lines 65-67, Col. 3)**. Therefore, it would have been obvious to modify Proctor, Gleichauf et al., and Hartley et al. with Brabson et al. to obtain the invention as specified in Claim 27.

d. *Referring to Claim 41:*

As per Claim 41, the rejection of Claim 39 is incorporated. In addition, Claim 41 encompasses limitations that are similar to those of Claim 27. Thus, it is rejected with the same rationale applied against Claim 27 above.

11. Claim 36 is rejected under 35 U.S.C. 103(a) as being unpatentable over Proctor (U.S. Patent 6,530,024) and Gleichauf et al. (U.S. Patent 6,301,668) as applied to claim 30 above, and further in view of Hartley et al. (U.S. Patent 6,889,168) and Brabson et al. (U.S. Patent 5,715,395)

a. *Referring to Claim 36:*

As per Claim 36, the rejection of Claim 30 is incorporated. In addition, Claim 36 encompasses limitations that are similar to those of Claim 27. Thus, it is rejected with the same rationale applied against Claim 27 above.

12. Claims 6-8, 18, 24 and 40 are rejected under 35 U.S.C. 103(a) as being unpatentable over Proctor (U.S. Patent 6,530,024), Gleichauf et al. (U.S. Patent 6,301,668), and Hartley et al. (U.S. Patent 6,889,168) as applied to claims 1, 13, 22, and 39 above, and further in view of Yang (U.S. Patent 6,467,002).

a. *Referring to Claim 6:*

As per Claim 6, Proctor, Gleichauf et al., and Hartley et al. disclose the method of claim 1. In addition, Gleichauf et al. disclose the step of conducting a discovery scan and a priority engine for prioritizing a plurality of analysis tasks. Gleichauf et al. do not expressly disclose assigning an asset value for the element, wherein the asset value indicates the relative importance of the element in the network. However, Yang discloses a priority assignment module for assigning priority values to various devices in the network environment **[i.e., Specifically, in one embodiment, the present invention assigns an initial priority order to the plurality of devices such tat those devices have**

priorities which are distinct (lines 44-46, Col. 2). Thus, the present invention is highly conducive for use with existing computer systems and/or networks (lines 4-6, Col. 10)]. Proctor, Gleichauf et al., Hartley et al., and Yang are analogous art because they are from similar technology relating to the computer system in the network. It would have been obvious to one of ordinary skill in the art at the time of invention was made to modify Proctor, Gleichauf et al., and Hartley et al. with Yang to have the function of the priority assignment module include in the priority engine since one would have been motivated to **realize that an efficient mechanism for priority arbitration is much needed in such a shred-resource environment in order to optimize the performance of computer systems and networks (lines 43-46, Col. 1, Yang)**. Therefore, it would have been obvious to modify Proctor, Gleichauf et al., and Hartley et al. with Yang to obtain the invention as specified in Claim 6.

b. *Referring to Claim 7:*

As per Claim 7, Proctor, Gleichauf et al., Hartley et al., and Yang disclose the method of claim 6. Proctor, Gleichauf et al., Hartley et al., and Yang do not expressly disclose the asset value is modified based on the audit scan. However, Proctor discloses the audit scan as in Claim 1. In addition, Yang discloses the priorities associated with the devices are subjected to modification

[i.e., Referring again to FIG 2A, in step 250, the priorities are reassigned among the devices (lines 48-49, Col. 6)]. Proctor, Gleichauf et al., Hartley et al., and Yang are analogous art because they are from similar technology relating to the computer system in the network. It would have been obvious to one of ordinary skill in the art at the time of invention was made to modify Proctor, Gleichauf et al., and Hartley et al. with Yang to have the function of the priority assignment module include in the priority engine since one would have been motivated to **realize that an efficient mechanism for priority arbitration is much needed in such a shred-resource environment in order to optimize the performance of computer systems and networks (lines 43-46, Col. 1, Yang)**. Therefore, it would have been obvious to modify Proctor, Gleichauf et al., and Hartley et al. with Yang to obtain the invention as specified in Claim 7.

c. *Referring to Claim 8:*

As per Claim 8, Proctor and Gleichauf et al., and Hartley et al. disclose the method of claim 1. Proctor, Gleichauf et al., and Hartley et al. do not expressly disclose the step of receiving a manually selected asset value for the element. However, Yang discloses that the priority value for the network element can be user-selected **[I.e., It is further appreciated that the initial priority order can be user designated (lines15-17, Col. 6)]**.

Proctor, Gleichauf et al., Hartley et al., and Yang are analogous art because they are from similar technology relating to the computer system in the network. It would have been obvious to one of ordinary skill in the art at the time of invention was made to modify Proctor, Gleichauf et al., and Hartley et al. with Yang to have the function of the priority assignment module include in the priority engine for receiving user input since one would have been motivated to **realize that an efficient mechanism for priority arbitration is much needed in such a shred-resource environment in order to optimize the performance of computer systems and networks (lines 43-46, Col. 1, Yang)**. Therefore, it would have been obvious to modify Proctor, Gleichauf et al., and Hartley et al. with Yang to obtain the invention as specified in Claim 8.

d. *Referring to Claim 18:*

As per Claim 18, the rejection of Claim 13 is incorporated. In addition, Claim 18 encompasses limitations that are similar to those of Claim 6. Thus, it is rejected with the same rationale applied against Claim 6 above.

e. *Referring to Claim 24:*

As per Claim 24, the rejection of Claim 22 is incorporated. Gleichauf et al. further disclose identifying an operating system for the network element **[i.e., Scan engine 22 can direct requests**

upon the network and assess responses to such requests to discover network information (lines 52-54, Col. 5). Such network information could comprise the devices coupled to internal network 10, the operating systems running on such devices (lines 59-61, Col. 5)]. In addition, Claim 24 encompasses limitations that are similar to those of Claim 4, 5, and 6. Thus, it is also rejected with the same rationale applied against Claim 4, 5, and 6 above.

f. *Referring to Claim 40:*

As per Claim 40, the rejection of Claim 39 is incorporated. In addition, Claim 40 encompasses limitations that are similar to those of Claim 4, 5, and 6. Thus, it is also rejected with the same rationale applied against Claim 4, 5, and 6 above.

13. Claims 10 and 19 are rejected under 35 U.S.C. 103(a) as being unpatentable over Proctor (U.S. Patent 6,530,024), Gleichauf et al. (U.S. Patent 6,301,668), and Hartley et al. (U.S. Patent 6,889,168) as applied to claims 1 and 13 above, and further in view of Yang (U.S. Patent 6,467,002) and Barroux (U.S. Patent 6,220,768).

a. *Referring to Claim 10:*

As per Claim 10, Proctor, Gleichauf et al., and Hartley et al. disclose the method of claim 1. Proctor, Gleichauf, and Hartley et al. do not expressly disclose remaining limitations of the claims.

However, Gleichauf et al. disclose identifying the function of the network element based on the discovery scan **[i.e., Scan engine 22 can direct request upon the network and assess responses to such requests to discover network information (lines 52-54, Col. 5). Such network information could comprise the devices coupled to internal network 10, the operating systems running on such devices, and services available on each device (lines 59-62, Col. 5)]**. Proctor discloses a policy for auditing **[i.e., Audit policy 300 (Fig. 3), which comprises of system audit, object audit, and registry key audit]**. Yang discloses a priority assignment module for assigning priority values to various devices in the network environment **[i.e., Specifically, in one embodiment, the present invention assigns an initial priority order to the plurality of devices such tat those devices have priorities which are distinct (lines 44-46, Col. 2). Thus, the present invention is highly conducive for use with existing computer systems and/or networks (lines 4-6, Col. 10)]**. Barroux discloses scheduling of tasks required for repetition. Proctor, Gleichauf et al., Hartley et al., Yang, and Barroux are analogous art because they are from similar technology relating to the computer system in the network. It would have been obvious to one of ordinary skill in the art at the time of invention was made to modify Proctor,

Gleichauf et al., Hartley et al. with Yang and Barroux to have the priority values associated to the network elements converted into repetitively scheduled tasks and associated the results with the policy disclosed by Proctor and the role by Gleichauf et al. since one would have been motivated to **realize that an efficient mechanism for priority arbitration is much needed in such a shred-resource environment in order to optimize the performance of computer systems and networks (lines 43-46, Col. 1, Yang)** and **to take advantage of SNMP (Simple Network Management Protocol) to collect survey information for a TCP/IP network (lines 10-12, Col. 2)**. Therefore, it would have been obvious to modify Proctor, Gleichauf et al., Hartley et al. with Yang and Barroux to obtain the invention as specified in Claim 10.

b. *Referring to Claim 19:*

As per Claim 19, the rejection of Claim 13 is incorporated. In addition, Claim 19 encompasses limitations that are similar to those of Claim 10. Thus, it is rejected with the same rationale applied against Claim 10 above.

Conclusion

14. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

a. Kingsford et al. (U.S. Patent 6,574,737) disclosea computer network penetration test discovers vulnerabilities in the network using a number of scan modules. The scan modules perform their scanning of the network separately but in parallel. A scan engine controller oversees the data fed to and received from the scan modules, and controls the sharing of information among the modules according to data records and configuration files that specify how a user-selected set of penetration objectives should be carried out. The vulnerability scan is initiated by a user who specifies what targeted network resources to scan. From that point on, the scan is data driven and models how an unwanted attacker would gain unauthorized access to the system.

b. Chang et al. (U.S. Pub. 2002/0112040) discloses a method, system, apparatus, and computer program product is presented for management of a distributed data processing system. A network management framework provides the ability to limit the frequency of discovery/scanning and/or monitoring on an endpoint-by-endpoint basis. A status polling interval can be dynamically determined for each endpoint throughout a highly distributed system whether or not the endpoints are situated behind routers, firewalls, slow communication links, etc. The monitoring operations can be set in accordance with a phase/life cycle of a performance monitoring component.

15. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Yin-Chen Shaw whose telephone number is 571-272-8593. The examiner can normally be reached on 8:15 to 4:15 M-F. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Yen Vu can be reached on 571-272-3859. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

YCS

Primary Examiner
Art Unit 2135

Jul. 1, 2005